AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions and listings of claims in the application:

1. **(Currently Amended)** A transceiver comprising:

an electrical interface configured to receive outgoing data signals from a host coupled to the transceiver and transmit incoming data signals to the host;

a fiber optic transmitter configured to transmit the outgoing data signals received from the host via the electrical interface;

a fiber optic receiver configured to receive the incoming data signals from an external device over a network communications channel; and

a controller configured to encrypt a string and supply the encrypted string to the [[a]]host via the electrical interface to authenticate the transceiver,

authentication of the transceiver being contingent upon whether or not the transceiver has been certified by a manufacturer of the transceiver and/or a supplier of the transceiver as meeting a specified quality standard.

2. **(Original)** The transceiver of claim 1, wherein the controller is configured to encrypt the string with a transceiver private encryption key.

3. **(Original)** The transceiver of claim 1, wherein the controller is configured to use a transceiver private encryption key and a transceiver public encryption key to authenticate the transceiver.

4. **(Original)** The transceiver of claim 3, wherein the controller is configured to encrypt the string with the transceiver private encryption key.

5. **(Original)** The transceiver of claim 3, wherein the transceiver public encryption key is sealed by encrypting the transceiver public encryption key with a system private encryption key and stored as a sealed transceiver public encryption key.

6. **(Original)** The transceiver of claim 5, wherein the sealed transceiver

public encryption key is decrypted with a system public encryption key to retrieve the transceiver public encryption key.

7. **(Original)** The transceiver of claim 1, wherein the controller comprises an electrically erasable and programmable read only memory that is used to store a transceiver private encryption key and a transceiver public encryption key.

8. **(Original)** The transceiver of claim 1, wherein the controller comprises a cryptography module for encrypting the string.

9. **(Original)** The transceiver of claim 1, wherein the controller comprises an RSA encryption module for encrypting the string.

10. **(Canceled)**

11. **(Canceled)**

12. **(Original)** The transceiver of claim 1, wherein the transceiver comprises a small form factor pluggable transceiver.

13. **(Currently Amended)** A network system comprising:

a host;

an interface electrically coupled to the host; and

a transceiver comprising:

a transmitter configured to transmit data signals;

a receiver configured to receive data signals; and

a controller configured to encrypt a string and to communicate the encrypted string to [[with]]the host through the interface to authenticate the transceiver with the host, authentication of the transceiver being contingent upon whether or not the transceiver has been certified by a manufacturer of the transceiver and/or a supplier of the transceiver as meeting a specified quality standard,

wherein the controller is configured to encrypt the string using a host-selectable one of a plurality of transceiver private encryption keys stored in the transceiver.

14. **(Original)** The network system of claim 13, wherein the interface comprises an inter-integrated circuit bus.

15. **(Original)** The network system of claim 13, wherein the interface comprises a transceiver fault status line.

16. **(Original)** The network system of claim 13, wherein the interface comprises a transceiver disable line.

17. **(Previously Presented)** The network system of claim 13, wherein the interface comprises a transmit data in line TD+ and an inverted transmit data in line TD-.

18. **(Previously Presented)** The network system of claim 13, wherein the interface comprises a received data out line RD+ and an inverted received data out line RD-.

19. **(Original)** The network system of claim 13, wherein the interface comprises a loss of signal status line.

20. **(Original)** The network system of claim 13, wherein the host is one of a mainframe computer, a workstation, a server, and a storage device.

21. **(Original)** The network system of claim 13, wherein the host is one of a bridge, a router, a hub, a local area switch and a wide area switch.

22. **(Currently Amended)** A transceiver comprising:

a transmitter configured and arranged to transmit data signals to an external device over a network connection in response to commands from a local host;

a receiver configured and arranged to receive data signals from the external device over the network connection and to pass corresponding data signals to the local host; and

a controller in communication with the transmitter and the receiver and configured and arranged to communicate with the local host over a local communication link to authenticate the transceiver with the local host, wherein the controller stores a first unique transceiver-specific public key/private key pair for authentication, the first unique transceiver-specific public key/private key corresponding with a manufacturer of the transceiver.

23. **(Previously Presented)** The transceiver of claim 22, wherein the first unique transceiver-specific public key/private key pair is associated with a first access code and the controller stores a second unique transceiver-specific public key/private key pair for authentication, wherein the second unique transceiver-specific public key/private key pair is associated with a second access code.

24. **(Previously Presented)** The transceiver of claim 23, wherein the first unique transceiver-specific public key/private key pair is used for authentication in response to the host communicating the first access code to the controller and the second unique transceiver-specific public key/private key pair is used for authentication in response to the host communicating the second access code to the controller.

25. **(Currently Amended)** A fiber optic transceiver comprising:

means for transmitting data signals to an external device over a network communications channel, the transmitted data signals being representative of data received from a local host;

means for receiving data signals from the network communications channel and transmitting corresponding signals representative of the received data signals to the local host; and

a controller configured to authenticate the fiber optic transceiver to the local host upon installation of the fiber optic transceiver without using the network communications channel, the controller enabling the host to determine whether or not the fiber optic transceiver is a cloned transceiver.

26. **(Original)** The fiber optic transceiver of claim 25, wherein the means for receiving data signals comprises means for converting optical serial data into electrical serial data.

27. **(Original)** The fiber optic transceiver of claim 25, wherein the means for transmitting data signals comprises means for converting electrical serial data into optical serial data.

28. **(Previously Presented)** The fiber optic transceiver of claim 25, wherein the controller is further configured to encrypt an authentication string using a transceiver specific private key, the encrypted authentication string configured to be decrypted using a transceiver specific public key.

29. **(Previously Presented)** A method for authenticating a transceiver in a system comprising:

installing a transceiver in the system so that the transceiver is in communication with a local host;

sending an authentication signal from the transceiver to the local host;

analyzing the authentication signal in the local host; and

selecting, at the local host, one of accepting and rejecting the transceiver based upon the analysis of the authentication signal, wherein:

the local host accepts the transceiver and uses the accepted transceiver for data communications with a remote external device over a network connection if the transceiver is determined by the local host to be authentic; and

the local host rejects the transceiver for data communications with the remote external device if the transceiver is determined by the local host to be inauthentic.

30. **(Original)** The method of claim 29, wherein the authentication signal comprises a certificate identification.

31. **(Original)** The method of claim 29, wherein analyzing the authentication signal comprises decrypting the authentication signal using a public key of an issuing authority.

32. **(Previously Presented)** A method for authenticating a transceiver, comprising:

plugging a transceiver into a corresponding receptacle of a local host to electrically couple the transceiver to the local host through a communication link, the transceiver comprising a transceiver specific public key/private key pair and the transceiver specific public key being encrypted with a private key of an issuing authority;

requesting, by the local host, the encrypted transceiver specific public key from the transceiver;

passing the encrypted transceiver specific public key from the transceiver to the local host by way of the communication link; and

decrypting the encrypted transceiver specific public key in the local host using a corresponding public key of the issuing authority to obtain the transceiver specific public key.

33. **(Previously Presented)** The method of claim 32 comprising:

generating an original authentication string in the local host;

sending the original authentication string from the local host to the transceiver;

encrypting the original authentication string in the transceiver using the transceiver specific private key;

passing the encrypted authentication string from the transceiver to the local host; and

decrypting the encrypted authentication string in the local host using the transceiver specific public key.

34. **(Original)** The method of claim 33 comprising:

comparing the decrypted authentication string to the original authentication string; and

selecting one of rejecting and accepting the transceiver based upon the comparison.

35. **(Original)** The method of claim 33, wherein the original authentication string is a random number.

36. **(Previously Presented)** The transceiver of claim 1, wherein if the transceiver is authentic, the transceiver cannot be cloned.